Description of SPARS Web User Roles[1]

SPARS users are given one of the roles described below, based on the type of work that they will be performing in SPARS. Every SPARS user has the following rights and restrictions:

Access Rights:
- o Able to change his/her password.
- o Able to obtain SPARS reports.

Access Restrictions:
- o Cannot delete or edit his/her SPARS account.
- o Cannot freely navigate through applications and inventories previously submitted to the AQB. However, the information in these is easily retrieved through the print-preview feature of SPARS Web.
- o Cannot delete or edit applications and inventories previously submitted to the AQB

1.0 Facility Administrator

Description: This account is created only by the AQB. The Administrator is responsible for creating and managing SPARS user accounts and passwords for his/her company's employees as well as for consultants. For companies with multiple facilities, a single Administrator may be identified for all the facilities, or an Administrator may be identified for each facility.

Access Rights:
- o Able to access the sites identified to the AQB on the _SPARS Access Request Form for Facility Administrators_.
- o Able to access application types assigned by the AQB.
- o Able to create applications and inventories.
- o Able to edit and delete applications and inventories as long as they are in INDUSTRY Phase.
- o Able to create, edit, and delete all other user roles.
- o Able to assign sites to all other user roles.
- o Able to reset a lost or forgotten password for all SPARS users, including his/her own.

Access Restrictions:
- o Cannot create, edit, or delete another Administrator.
- o Cannot generate a personal identification number for a Responsible Official.

---

[1] The following roles are no longer used: "Facility Super User" and "Facility Viewer."

2.0 Facility User

Description: This account may be created by Administrators, Super Users, or the AQB.

Access Rights:
- o Able to access the sites and application types assigned by the Administrator, the Super User, or the AQB.
- o Able to create applications and inventories.
- o Able to edit and delete applications and inventories as long as they are in INDUSTRY Phase.
- o Able to change his/her password.

Access Restrictions:
- o Cannot create, edit, or delete an Administrator, a Super User, a Viewer, or another User.
- o Cannot assign or delete sites for an Administrator, a Super User, a Viewer, or another User.
- o Cannot generate a personal identification number for a Responsible Official.
- o Cannot reset a lost or forgotten password.

3.0 Responsible Official

Description: This account is created only by the AQB. The *SPARS Access Request Form for Responsible Officials* submitted to the AQB includes the Responsible Official's signature, which carries the same legal weight and responsibility as the signature on the paper Form FI or Part 3.

Access Rights:
- o Able to access the sites identified to the AQB on the *SPARS Access Request Form for Responsible Officials*.
- o Able to access the application types assigned by the AQB.
- o Able to submit applications and inventories to the AQB. To be able to do this, the Responsible Official is issued a personal identification number, which must be entered while logged in as the Responsible Official.
- o In addition to these, the Responsible Official can have the access rights of any of the above user roles. Normally the AQB assigns a Facility User role to Responsible Officials, unless they are also the Facility Administrator, in which case, the AQB creates them as Administrators.

Access Restrictions:
- o Because the AQB normally assigns a Facility User role or a Facility Administrator role to Responsible Officials, their access restrictions will be the same as those of a Facility Administrator or a Facility User.